IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF NEW MEXICO

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	Case No. 5:15-CR-3386-RB
vs.	)	
	)	
JOSEPH RAY MENDIOLA,	)	
	)	
Defendant.	)	

UNITED STATES' RESPONSE TO DEFENDANT JOSEPH RAY MENDIOLA'S MOTION TO SUPPRESS

On August 19, 2016, Defendant Joseph Ray Mendiola filed a Motion to Suppress Physical Evidence and Oral Statements (Doc. 227). In his Motion, Defendant seeks to suppress evidence collected from a wiretap that the United States obtained pursuant to Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III"). He argues that the affidavit in support of the wiretap application included information that the United States could not have obtained lawfully.

Defendant's argument is substantively and procedurally flawed. Substantively, Defendant's vague allegations about the United States illegally obtaining information are false. The United States legally obtained the information that Defendant calls into question. Procedurally, Defendant cannot invoke the remedy of suppression because he alleges a violation of the Electronic Communications Privacy Act ("ECPA"), not Title III. The ECPA does not provide suppression as a remedy for violations of its provisions. Finally, even if a Title III violation occurred, the intercepting agents acted in good-faith reliance upon the Court's order

authorizing interception. For each of these reasons, the Court should deny Defendant's Motion (Doc. 227).

I. Relevant Background

On September 22, 2015, Defendant was charged in nineteen of twenty-four counts in a federal indictment relating to his leadership of a drug-trafficking organization operating in Roswell, New Mexico. *See* Doc. 48. During the investigation leading to those charges, the United States sought and obtained a court order allowing the United States to intercept wire and electronic communications from a cellular phone labeled Target Telephone 1. *See* Ex. A (Sealed Ex Parte Application for Interception of Wire and Electronic Communications, Affidavit in Support of Application, and Order Authorizing Interception of Wire and Electronic Communications, District of New Mexico Case Number 15-MR-353-RB).[1] Law enforcement agents had reason to believe that Target Telephone 1 belonged to Gerald Sentell, a distributor working with Defendant in Roswell. *Id.* at 5.[2]

To establish probable cause in support of the wiretap application, the United States partly relied on information gained from and activities conducted by a confidential source labeled CS1. *See id.* at 13. Among those activities was a controlled purchase of methamphetamine that CS1 conducted. *See id.* at 31. On March 31, 2015, CS1 purchased 28.9 grams of methamphetamine from Sentell and recorded the transaction. *Id.* After the transaction, and under the direction of law enforcement agents, CS1 called Sentell on Target Telephone 1 to inquire about another

[1] Exhibit A is not attached hereto given the file-size restrictions of attachments uploaded to CM/ECF. The Court may access the Application, Affidavit, and Order on the docket in Case Number 15-MR-353-RB, and the United States has produced these documents to Defendant in discovery.

[2] The page numbers contained in the citations to Exhibit A herein will refer to the page number at the bottom of the Affidavit in Support of Application.

methamphetamine purchase, and Sentell agreed to another sale. *Id.* Agents observed CS1 make the call and dial the digits comprising the phone number for Target Telephone 1. *Id.*

The United States also relied on information derived from a pen register and trap and trace device ("pen/trap") on Target Telephone 1 to establish probable cause for the wiretap. *See id.* at 70. The United States obtained a court order on April 3, 2015, permitting installation of the pen/trap. *Id.*; *see also* Ex. B (Ex Parte Application and Ex Parte Order, District of New Mexico Case Number 15-MR-190). The United States' affidavit in support of an application for a wiretap included an analysis of information derived from the pen/trap. Ex. A at 37. Specifically, the affidavit recounted calls and messages between Target Telephone 1 and phone numbers associated with 1) Jax Martinez, an individual who participated in various methamphetamine transactions conducted by a confidential source, 2) Brandy Matthewson, an individual suspected of trafficking methamphetamine based on information obtained from a confidential source, and 3) Rodney Boughton, an individual who sold methamphetamine to a confidential source and trafficked methamphetamine with Sentell. *Id.* at 37–40. The pen/trap was not installed on Defendant's phone, and it did not intercept any information about calls or messages to or from Defendant that the United States used in its wiretap affidavit.

II. Legal Standard

An "aggrieved person" may move to suppress the contents of communications intercepted on a Title III wiretap by showing: "(i) the communication was unlawfully intercepted; (ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or (iii) the interception was not made in conformity with the order of authorization or approval." 18 U.S.C § 2518(10)(a). "A defendant bears the burden of proving that a wiretap is invalid once it has been authorized." *United States v. Barajas*, 710 F.3d 1102,

1107 (10th Cir. 2013) (quoting *United States v. Ramirez-Encarnacion*, 291 F.3d 1219, 1222 (10th Cir. 2002)).

III. Argument

a. Defendant's factual allegation misses the mark.

To begin, Defendant's entire Motion rests on a speculative factual assertion that is entirely false. Although his argument is not entirely clear, Defendant seems to assert that the March 31, 2015, controlled buy outlined in the wiretap affidavit somehow could not have occurred unless the United States had information about Target Telephone 1 gleaned from a pen/trap. Because the United States did not obtain an order authorizing a pen/trap on Target Telephone 1 until April 3, 2015, Defendant speculates that the United States must have employed an unlawful pen/trap.

The inference that Defendant draws is puzzling. The affidavit's account of the March 31 controlled buy is as follows:

> On March 31, 2015, CS1 purchased 28.9 grams of methamphetamine from Sentell for $800 at No Name Residence. Under the direction of agents, CS1 recorded the transaction. While the audio is of poor quality, the video contains clear images of Sentell and the methamphetamine. After the deal, under the direction of agents, CS1 called Sentell on **TARGET TELEPHONE 1** to ask Sentell the price of a quarter pound of methamphetamine. Sentell replied $2800 and said he had it. Agents observed CS1 make the call and dial the digits, but did not have equipment on hand to record Sentell's participation in the call.

Ex. A at 31. These events do not lead to the conclusion that the United States must have employed an unlawful pen/trap. The United States had been investigating Sentell since June of 2014. *Id.* at 5. The United States had spoken with eleven different confidential sources, including CS1, who had access to the organization to which Sentell belonged. *Id.* at 13–19. In fact, CS1 had conducted a deal with Sentell three weeks before the March 31 controlled buy. *Id.* at 31. Although Defendant is correct that the March 31, 2015, controlled buy is the first mention

of Target Telephone 1 in the wiretap affidavit, it makes perfect sense that CS1 would know Sentell's phone number. And, as the wiretap affidavit states, the agents physically watched CS1 dial Sentell's phone number (i.e., Target Telephone 1) immediately after the March 31, 2015, controlled buy. *Id.*

Defendant states that the "only plausible explanation for how Agent McGuire could have this information is that he was referring to subscriber information provided by the cellular telephone company." Doc. 227 at 4. The United States did in fact have subscriber information for Target Telephone 1 prior to March 31, 2015, but Defendant is incorrect that "[t]he government had no authorization to have this information on March 31, 2015."[3] *See id.* A telephone provider must produce subscriber information and other basic information for a particular telephone number when served with an administrative subpoena issued by a federal law enforcement agency. 18 U.S.C. § 2703(c)(2). On February 26, 2015, FBI Special Agent Colin McGuire served an electronic administrative subpoena on AT&T seeking the subscriber information for Target Telephone 1, and the FBI received the information that same day. Ex. C (Administrative Subpoena Issued to AT&T on February 26, 2015). This was lawful under 18 U.S.C. § 2703(c)(2). Therefore, Defendant's allegation that the United States must have unlawfully obtained subscriber information for Target Telephone 1 is entirely false.

[3] The wiretap affidavit itself reveals that the United States had obtained the subscriber information and that the subscriber information was entirely unrelated to anything that happened with the March 31, 2015, controlled buy. The affidavit states that "[r]ecords from AT&T show that **TARGET TELEPHONE 1** is subscribed to 'PREPAID CUSTOMER' at address 1234 Gophone Way, Roswell, New Mexico 88203." Ex. A at 5; *see also* Ex. C at 6. This is obviously fake information, and it further emphasizes the faulty nature of Defendant's inference. The United States could have, and in fact did, conduct the March 31, 2015, controlled buy without true subscriber information.

b. Defendant alleges a violation of ECPA, not Title III, so he cannot seek to suppress any evidence based on his allegations.

Even if his factual allegation were true, Defendant does not allege that the communications he seeks to suppress were intercepted unlawfully under any of the provisions in Title III. He also does not allege that the United States' affidavit in support of its application for a wiretap contained any material misstatements or omissions. Rather, he alleges that the affidavit in support of the application to intercept those communications contained information that the United States "could not have legally had in" its possession unless it had employed an unlawful pen/trap. He then makes an unwarranted jump by arguing that use of an unlawful pen/trap in this case would mandate exclusion under Title III in spite of the fact that ECPA, not Title III, governs the use of pen/traps. *See* Doc. 227 at 3 ("It is a violation of federal law to employ a pen register or trap and trace device without court authorization. 18 U.S.C. § 3121(d). While the pen register and trap and trace statutes themselves do not codify the exclusionary rule, Title III specifically mandates exclusion of all direct and derivative evidence obtained as the result of an illegal wiretap. 18 U.S.C. § 2515 and § 2518(1)(a)."). But if Defendant only alleges a violation of ECPA's provisions and not Title III's, then he is limited to the remedies available under ECPA. Suppressing the fruits of a violation is not one of them.

Pen/traps differ significantly from wiretaps in that they "do not acquire the *contents* of communications. . . . Indeed, a law enforcement official could not even determine from the use of a pen register whether a communication existed. These devices do not hear sound." *See Smith v. Maryland*, 442 U.S. 735, 741 (1979) (internal quotation marks and citation omitted). Rather, a pen register reveals which phone numbers the target phone contacts while a trap and trace device reveals which phone numbers contact the target phone. *In re Application of the U.S.*

for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, 890 F. Supp. 2d 747, 750–51 (S.D. Tex. 2012).

Accordingly, wiretaps and pen/traps are governed by separate laws. Wiretaps are governed by Title III, 18 U.S.C. § 2510 *et seq.*, and pen/traps are governed by ECPA, 18 U.S.C. § 3121 *et seq.* To intercept the contents of a wire, oral, or electronic communications with a wiretap, the United States must file an application with a federal judge seeking an order authorizing the wiretap under 18 U.S.C. § 2516, and the judge may grant the application if the United States has met the requirements enumerated in 18 U.S.C. § 2518(3). If the contents of a wire, oral, or electronic communication are intercepted without obtaining an order or without meeting these requirements, Title III specifically provides that an "aggrieved person" may move to suppress the contents of the communication or any evidence derived therefrom. 18 U.S.C. § 2518(10)(a).

To install a pen/trap, the United States must first apply for a court order pursuant to 18 U.S.C. § 3122, and the court must grant such an order under 18 U.S.C. § 3123 if the United States has certified that the information likely to be obtained by the pen/trap is relevant to an ongoing criminal investigation. However, using a pen/trap without abiding by the procedures in ECPA cannot, by itself, result in any suppression of evidence. As a constitutional matter, installing a pen/trap without court approval cannot lead to suppression under the Fourth Amendment and its associated exclusionary rule because installing a pen/trap is not a search within the meaning of the Fourth Amendment. *United States v. German*, 486 F.3d 849, 852–53 (5th Cir. 2007) (citing *Smith*, 442 U.S. at 735). As a statutory matter, 18 U.S.C. § 3121(d) only provides criminal penalties for violating ECPA's pen/trap provisions. Simply put,

"[s]uppression of evidence is not a remedy for alleged violations of the ECPA."[4] *United States v. Stegemann*, 40 F. Supp. 3d 249, 271 (N.D.N.Y. 2014) (quoting *United States v. Navas*, 640 F. Supp. 2d 256 (S.D.N.Y. 2009)).

In his Motion, Defendant alleges a violation of ECPA and nothing more. He does not allege that the United States intercepted the challenged communications without obtaining an order under Title III or without meeting the statutory requirements. He does not allege that the order authorizing the wiretap was the product of material misstatements in or omissions from the affidavit supporting the application. Rather, he alleges that the United States employed an unlawful pen/trap. Even if that allegation were true, which it is not, it would constitute a violation of ECPA and not Title III. Because suppression of evidence is not a remedy for an ECPA violation, Defendant's allegation cannot give rise to the remedy he seeks.[5]

---

[4] Although Defendant facially seems to argue that the United States obtained information via use of an unlawful pen/trap, parts of his Motion assert that the United States unlawfully obtained subscriber information for Target Telephone 1. *See* Doc. 227 at 4. Obtaining subscriber information from a telephone provider is governed by a different part of ECPA called the Stored Communications Act ("SCA"), and "the SCA 'allows for civil damages, *see* 18 U.S.C. § 2702, and criminal punishment, *see* 18 U.S.C. § 2701(b), but nothing more. Indeed, the [SCA] also expressly rules out exclusion as a remedy; Section 2708, entitled 'Exclusivity of Remedies,' states specifically that § 2707's civil cause of action and § 2701(b)'s criminal penalties 'are the only remedies and sanctions for violations of' the [SCA].'" *United States v. Bermudez*, No. IP 05-43-CR-B/F, 2006 WL 3197181, at *8 (S.D. Ind. June 30, 2006) (quoting *United States v. Smith*, 155 F.3d 1051, 1056 (9th Cir. 1998)).

[5] It is also worth noting that even if Defendant could somehow use Title III's suppression provision to remedy an ECPA violation, Defendant's argument would fail under Title III's standing principles. Title III's suppression provision only allows an "aggrieved person" to seek suppression of evidence. 18 U.S.C. § 2518(10)(a). "Although Title III contains this express standing provision, courts have long recognized that Congress's intent was to apply the existing law of Fourth Amendment standing to wiretap cases." *United States v. Martin*, 169 F. Supp. 2d 558, 564 (E.D. La. 2001) (citing *Alderman v. United States*, 394 U.S. 165 (1969)). "Standing under the Fourth Amendment is narrowly construed to include only those whose privacy rights are actually violated," and this means that a person may only move to suppress a certain communication under Title III if he was a party to that particular communication. *See id.* at 565–66 (stating that because the defendant "was not an interceptee in the . . . conversations [from a

c. Even if a Title III violation occurred, the intercepting agents acted in good-faith reliance upon the Court's order authorizing interception.

Finally, even assuming a Title III violation occurred, the Court should not suppress the communications that agents intercepted on the wiretap because the agents acted in good faith based on the authorizing order. In the Fourth Amendment context, the good-faith exception counsels that a court should not suppress evidence that resulted from an unlawful search or seizure when the acting agents "have acted in an objectively reasonable manner by relying on a warrant issued by a neutral and detached magistrate." *United States v. Herrera*, 444 F.3d 1238, 1249 (10th Cir. 2006). Whether the good-faith exception that applies to the exclusionary rule associated with the Fourth Amendment also applies to suppression under Title III when an agent reasonably relies on an order authorizing a wiretap is an open question in the Tenth Circuit. *United States v. Barajas*, 710 F.3d 1102, 1110 (10th Cir. 2013) (declining to decide the issue and noting a circuit split between the Fourth, Eighth, and Eleventh Circuits, which have held that the good-faith exception does apply in the Title III context, and the Sixth Circuit, which has held that it does not). However, the rationale underlying the good-faith exception in the Fourth Amendment context applies even more strongly in the Title III context. Namely, excluding evidence when agents have reasonably relied on an order authorizing a wiretap would not deter misconduct in obtaining wiretaps, and applying a good-faith exception would not increase agents' use of wiretaps. *See generally* Derik T. Fettig, *When "Good Faith" Makes Good Sense:*

---

prior wiretap] that provided probable cause for the subsequent [wiretap] and had no privacy interest in those conversations, he would have no standing to suppress them directly").

So, even if Defendant could somehow carry Title III's suppression provision over to an ECPA violation, he would lack standing. The allegedly unlawful pen/trap was not installed on Defendant's phone, and none of the information in the affidavit from the pen/trap came from communications that he had with Sentell. Therefore, he could not argue that the wiretap issued as a result of violating *his* rights under ECPA.

Applying Leon*'s Exception to the Exclusionary Rule to the Government's Reasonable Reliance on Title III Wiretap Orders*, 49 HARV. J. ON LEG. 373 (2012).

Here, agents reasonably relied on the Court's authorizing order when intercepting the communications that Defendant seeks to suppress. The Court's order was facially valid, and the United States' affidavit in support of its application included all of the information that Defendant relies upon to infer that the United States possessed certain information unlawfully. A reasonable agent would believe, based on the fact that the affidavit included this challenged information, that the Court's issuance of an authorizing order meant that the agent could intercept communications under the circumstances. Therefore, even assuming a Title III violation occurred, the Court should not suppress the challenged communications because of the violation.

IV. Conclusion

For the reasons above, the Court should deny Defendant's Motion to Suppress Physical Evidence and Oral Statements (Doc. 227) without an evidentiary hearing because he has failed to meet even his threshold burden of showing a Title III violation.

Respectfully submitted,

DAMON P. MARTINEZ
United States Attorney

Electronically filed 9/16/2016
RANDY M. CASTELLANO
JOHN A. BALLA
Assistant United States Attorneys
555 S. Telshor, Ste. 300
Las Cruces, NM 88011
(575) 522-2304 – Tel.
(575) 522-2391 – Fax

I HEREBY CERTIFY that I filed the foregoing motion electronically via CM/ECF which will cause this motion to be delivered to counsel for defendant.

Electronically filed September 16, 2016
JOHN A. BALLA
Assistant United States Attorney